Author: ROBERT$S@SMTP (Robert Sullivan) {Robert_Sullivan@ccm.sc.intel.com} at MHS
Date: 7/10/96 04:20 PM
Priority: Normal
TO: Fritz Attaway at MPAA-DC
CC: MICHAEL$@SMTP {Michael_Moradzadeh@ccm.sc.intel.com} at MHS
Subject: document per our discussion
---------- Message Contents ----------

To: fattaway@mpaa.org
Cc: Michael_Moradzadeh@ccm.sc.intel.com
From: Robert Sullivan <Robert_Sullivan@ccm.sc.intel.com>

High-level Summary - Intel DVD Copy Protection Proposal

draft/not for distribution - Rob Sullivan, July 9th, 1996

Voluntary "Contract" Model & Encryption/Decryption

- When content is encrypted the playback system must participate actively to obtain the keys and to initiate decryption of the title. If it does not, the DVD-Movie drive would not pass the title and/or pressing unique decryption keys to the player, and the encryption would hide the protected content.
- A voluntary "contract" would exist between makers of DVD-Movie player devices and those who distribute protected titles. Unique authentication "credentials" in the form of digitally signed certificates would be given only to player devices which commit to implement completely compliant copy-protection behavior. Manufacturers who choose not to support protected DVD-Movie format could still ship DVD-ROM devices which are not able to read protected files or keys.
- The voluntary "contract" terms could change over time as economic, legal, and technical protections evolve.
- The terms would define "compliance" for the devices which would receive playback authorization credentials. The terms must obviously be non-discriminatory and non-exclusive at all times to prevent anti-trust exposure - hence the processes for modifying these terms would be cumbersome but manageable.
- "Compliant" copy protection behavior should include CGMS-like copy management as described in the original DVRA draft and would address digital-to-digital, digital-to-analog, and analog-to-digital cases.
- "Compliant" copy protection behavior should include a requirement to faithfully carry the "protected" copy protection status mark forward. This mark for analog (NTSC or PAL) would be CGMS-A and Macrovision's ColorStripe, so a transformation from digital to analog would require the analog mark if digital source content is protected. A mutually agreeable transition period to accommodate incorporation of analog protection signals (such as Macrovision) into current PC hardware would be required.
- After the transition period PC graphics devices that cannot affirm compliance might be assumed *not* to correctly handle analog RGB signals or to generate Macrovision APS signals. To limit analog RGB circumvention, the system software could then refuse to play protected DVD-Movies full screen or with NTSC/PAL compatible timing. A movie in a operating system user interface "window" on part of the screen would be less valuable to one considering circumvention. Non standard analog RGB output timing would mean that inexpensive and generally available RGB to NTSC/PAL converters could not be used to circumvent copy protection - the output would not be recordable on a standard VCR.

Key Management Hierarchy

- Our technical teams have converged on cryptographic "Best Known Methods" for key management and key exchange. The MPAA and the DVD Consortium will need to architect processes for creation and conditional distribution of the necessary credentials for compliant DVD-Movie drives and player devices. Studios will need a way to get signed encryption keys for each title/pressing also.
- An entity - existing or new - could also administer the terms of the voluntary "contract" and would grant unique signed credentials and keys to parties on the basis of "contract" compliance.
- DVD-Movie drives would be able to read the "hidden" decryption keys from the DVD-Movie titles. DVD-Movie drives would verify the credentials of authorized devices by using the public

key of the administration entity described above. Without authorization, decryption keys would not be released by the DVD-Movie drive.

- Devices requesting keys from a DVD-Movie drive would present the credentials obtained under license from the key management entity - after authentication the drive would pass the keys to the decryption function in the player using a secure handshake.

Specified System-Level Behavior

- Desired copy protection functionality would be described at the system level, independent of specific product implementations.
- The encryption algorithm and protected DVD-Movie format, for example, would be described in the DVD specifications. The interface command-set for DVD drives could also be "standardized" and described in these specifications. PCs and other devices would use these interfaces to implement the authentication and key exchange functions which enable actual playback. Existing software including file copy and drag-and-drop copy functionality would not be aware of the new device commands and thus would not be able to copy protected DVD-Movie files.
- Certain aspects of the DVD-Movie format might remain a trade-secret among the DVD licensees. The location and encoding of the hidden keys on DVD-Media, for instance, would not need to be known by anyone but DVD-Movie drive implementers, and the information could be delivered under license along with required keys from the key management entity.

Innovation Must Be Enabled for Specific Product Implementations

- Allow the actual engineering design (within bounds of a functional specification) to companies which build products.
- Innovation could yield more robust and lower cost implementations of the copy protection scheme over time. This innovation could be reinforced or encouraged over time to counter the increasing economic incentives for copying due to decreases in blank DVD recordable/removable media.

Legislative Principles

Generally a circumvention definition that comprehends the voluntary contract and conditional authorization aspects of our model could greatly simplify the legislative concepts and hence accelerate the legislative process.

- Derivation (through brute force cryptographic attack) or distribution of decryption keys or authorization credentials when a reasonably foreseeable effect is to enable infringement of copyright holder's rights should be illegal.
- Presentation of use authorization credentials by a person or device other than which was specifically authorized by the copyright holder should be illegal.
- Any device which has the primary purpose or effect of circumventing lawful copy protection means should be illegal. This could be accommodated in a bill not unlike the proposed H.R. 2441 draft NII legislation.
    - The encryption and the voluntary "contract" model make the definition of circumvention very clear, at least in the digital-to-digital case. We believe that this makes the difference between primary purpose and reasonably foreseeable effect negligable- this thesis obvioiusly needs to be tested.
    - A pass-through device which converts analog RGB to NTSC/PAL *and* which samples and re-times the signal arguably has the primary purpose or effect of circumvention. Inexpensive and currently available RGB to NTSC converters simply would not work due to non-standard timing.
- Contributory infringement, royalties for technology or devices required for compliance, and anti-trust immunity must be comprehended but are not addressed in this document.

M-23074

OUTSIDE COUNSEL'S EYES ONLY

Strawman Copy Protection Legislation Thoughts

(from Moradzadeh, I'll review with Fritz Attaway on Wednesday)

Goals

- Prevent distribution of devices which are aimed at illegal copying.
- Support technical solutions with legislative protection of critical elements.
- Accommodate new policies, such as home taping, where appropriate.

Basic Principles

- *Protection of Investment is Good.* - IP laws encourage innovation and investment.
- *Engineers Work Faster than Lawyers.* - As new problems arise, technical solutions will often come faster and cheaper than legal ones.
- *Less Law is Better Law.* - A simple law will be easier to adopt and to adapt to changing circumstances.
- *Self Help First.* - Content which makes no effort to "protect itself" gets the benefit of basic copyright law. Content which uses some means to protect itself gets additional legal protection for its method.

1. Support for Technical Solutions.

IF we can predict an industry consensus on likely protection means, then legislation which protects those means is appropriate. Based on current discussions, two provisions are suggested. These are **not** "primary purpose" tests. If the conditions are met, the device or product is illegal:

1A *False Keys.* A prohibition on the distribution or creation of decryption keys where a reasonably foreseeable effect is to permit the unauthorized violation of specified rights of a copyright holder.

1B *False Impersonation.* A prohibition on devices which falsely identify themselves as "honest products." This term would require more definition, but would essentially mean products which comply with predefined rules on serial copying, transmission, etc.

These provisions would apply to any industry-adopted means, or even to a proprietary solution.

2. Fall-Back Anti-Circumvention Provision.

Where the above general prohibitions don't apply, a device could still be prohibited. A simple provision should prohibit devices and services which have a **primary purpose or effect** of circumventing lawful copy protection means. This would disallow Macrovision scrubbers etc. The text of such a bill would be about the same as originally proposed for SB 2441.

M-23075

3. Accommodate Policies.

The PC industry has not expressed a position on the various compromises reached with respect to home copying. Provisions allowing certain numbers of copies in certain circumstances and prohibiting application of these rules to unprotected works are acceptable to Intel, and legislation implementing these compromises is appropriate either in a bill such as is contemplated here or elsewhere.

Intel DVD Copy Protection Proposal

Strawman #1 - July 2nd, 1996

1. Specified copy protection scheme does not constrain implementation to software or hardware- simply specifies system level behavior, particular DVD-Movie format components related to encryption keys, encryption algorithms. Consumers benefit from the innovation that is hence enabled - and we share an incentive to make the technical level of protection stronger with successive implementations over time.
2. We assume all three industries (MPAA, Consumer Electronics, PC industry) will cooperate on legislative package to balance technical vs. legal and economic means of protection.
    - Specifically we agree to support legislation which makes circumvention and distribution of "primary purpose" circumvention technology illegal whether implemented in software or hardware.
    - Other legislative needs to be determined by policy group but will likely include immunity from contributory infringement for compliant devices, should address patent/royalty issues for compliant implementations, etc.
    - Some parties feel strongly that an accredited standards body needs to codify the "standard" to win anti-trust immunity for this copy protection effort. Intel believes that an "open-process" private standard with clear non-discriminatory purpose and license terms is sufficient as it is with other PC industry standards. Intel will cooperate fully with any formal standards initiative but we won't wait indefinitely for a standards body to act.
3. Proposed PC O/S Specifics:
    - Early (late '96?) operating system releases would support play for DVD-Movie disks but would not support copy functions (drag-drop, stdio read(), etc.) for DVD-Movie disks. New stdio read() functions and device commands for protected data, as well as device commands for key exchange with DVD-Drives would be defined and implemented.
    - Initial DVD-Movie player application (in cooperation with other system software per individual OSV decisions) would implement key exchange and decrypt/decompress control (via media subsystem in O/S). Stream analysis, decryption, and media decompression would be abstracted to enable equivalent implementation in either software or hardware.
    - Operating system releases to follow (as reasonably possible) would include greater software tamper-resistance (across subsystems required for DVD-Movie play) and would support early Analog output Macrovision/APS enabled hardware as available.
    - At some point in time full screen playback of DVD-Movie might not be allowed to NTSC/PAL outputs that do not implement Macrovision/APS; could consider similar constraints even for analog-RGB to limit exposure due to cheap analog-RGB to NTSC/PAL converters. Device qualification via Plug & Play attributes or the equivalent thereof in other operating environments could be used.

4. The final scheme should allow production of protected DVD-Movie disks (writeable media) on PC which play in standalone players *but* the protection scheme does not need to be the same as that of stamped (mass-produced) media.
5. Cross-industry effort is still required to define "interlocks" which maximize protection of protected content. MPAA protected DVD-Movie content on PC writeable media could still be rejected - should not be mountable on PC DVD-Rom drives, for instance.
6. Regionalization: implemented in Operating System software (specifically not in the drives) and based on install time or first time use/setup query to user.
    - Could require O/S re-install to change regions (make it inconvenient at least for user to change regions, make US region unable to play non-English language disks (?) so user would need to choose a region and stick with it).
    - Number and borders of regions might be arbitrary, should be able to define with MPAA as required. Assume different OSVs have different support regions, assume it would be hard to sustain any attempt at mapping regions onto every OSV's support regions, etc.
7. Time Shifting: keep all of the defined CGMS states (0/0, 0/1, 1/0, etc) including the one that allows time shifting or "one generation" copies in the ROM media case. Its a content provider option to use any or all of the CGMS encodings. At least we - the computer industry - enabled time-shifting and we don't get blamed for taking it away from consumers (was this the CEMA motivation for keeping this in DVRA??). Over time we assume copy management will evolve to a more robust "rights description" language and container technology - which will subsume CGMS. This works for now.
8. Digital to Analog: given a manageable design/procurement transition period, PCs would include ability to generate Macrovision/APS signals on all PAL/NTSC analog outputs. Tamper-resistant O/S software (possibly the DVD-Movie player app?) would turn this on as required by the logic definitions in the DVRA TRD draft or something very similar.
9. Analog to Digital: Still <tbd>, but should be ok with a longer transition period to allow resolution of additional design issues. PC NTSC/PAL video capture should detect Macrovision/APS (and/or CGMS-A on VBI?) and implement correct copy protection behavior for protected video inputs. Desired effect would be to disallow capture/compress/copy of protected analog video inputs.
10. Watermarks
    - Indelible atermark that is easy (cheap) to read/detect would be a nearly ideal method for keying copy protection/management behavior - including control of Macrovision/APS signals on NTSC/PAL and even analog-RGB outputs, as "protected data" indicator for copy management logic in O/S.
    - No such technology (indelible + cheap to detect in '96/'97 timeframe) has been presented. Given the current progression of CPU performance (Moore's Law) watermark detection could be implemented along with soft decode in 2-4 years however.
    - If we define and include such a watermark in media streams from the beginning we could enable later enhancements to the security of DVD-Movie copy protection systems when host CPU (or DSP, etc).
    - This method - and phased implementation based on CPU cycles available over time - could be the answer to the RIAA & digital audio problems. Need to investigate.

M-23078